Our Docket No: 42P11579C2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)		
	)		
Gibbs et al.	)	Examiner:	Song, H.
	)		
Application No: Not yet assigned	)	Art Unit:	2131
	)		
Filed: Concurrently Herewith	)		
	)		
For: <u>Unique Digital Signature</u>	)		

PRELIMINARY REMARK

Mail Stop: Patent Application
Commissioner for Patents
P.O Box 1450
Alexandria, VA 22313-1450

Sir:

Prior to the examination of the present application, Applicants respectfully request the

Examiner to consider the following remark.

<center>**Remark**</center>

<center>**35 U.S.C. §103 Rejection**</center>

<center>*Ginzboorg in view of Dancs et al.*</center>

The Examiner has rejected claims 32-41 and 58-60 of the parent application under 35

U.S.C. §103 (a) as being unpatentable over Ginzboorg et al., U.S. Patent No. 6,240,091

("Ginzboorg") in view of Dancs et al., U.S. Patent No. 6,112,305 ("Dancs"). As for Claim 1, the

Examiner relies on Ginzboorg at Col. 8, lines 12-48 and upon Dancs at Col. 8, lines 31-42. These

rejected claims of the parent application correspond roughly to Claims 1-22. Ginzboorg, however

has at least no teachings that are relevant to the following claim recitations (of Claim 1, many of

which are also in independent Claim 13):

[a] digital signature created using a one-way hash function

a one-way hash function having an index number... as inputs

the unique digital signature is configured to be successfully authenticated no more than a

fixed number of times

the fixed number of times corresponding to the index number

Dancs states only that "this digital signature is used only once for verification at the time of

writing....the digital signature is then discarded." There is no one-way hash function, no index

number and no fixed number of times (unless that number is one). There is nothing about the

signature that has any affect on whether the signature is discarded nor on how often it is used. In

addition, this discarding of the signature is applied only to information to be stored in the RAM or

NVRAM.

The effect of the suggestion in Dancs is also significant. In Dancs, after the information is verified using the signature, then the information is stored in the clear (with no security). "The inside of the NC client is deemed to be tamper proof for the purposes of the NC client's security requirements." The Examiner suggests that the one time verification in Dancs enhances security and frustrates outsiders by frequently changing the signature. Dancs suggests just the opposite. In Dancs, security is reduced because after being checked once, any third party with access to the NC can gain any desired information. After the signature is discarded, it is not replaced with another, the information is stored in the clear.

Applying Dancs to the teaching of Ginzboorg would provide that digests for charging records get sent with signatures, encrypted using a private key (8:47-50). The digests would then be decrypted using the public key and either discarded (authentication being complete) or stored with the charging record in the clear.

On page 2 of the action, the Examiner writes that it would have been obvious... to use a fixed number authentication and deletion method... because a digital signature can only be authenticated a fixed number of times and then discarded after its use, digital signatures are not repeated and are non-deterministic so that third parties or intruders cannot replay the information. Further.. an unauthorized user cannot reuse a digital signature he/she found or stole from an authorized user because it changes each time the user wishes to be authenticated, therefore security is greatly enhanced by using this method.

This suggested motivation for combining the two references to obtain the invention of the present application does not come from either reference. In Ginzboorg, the object is to verify the source of a message, not to ensure the security of the message (8:38-41). In Dancs, the object is to secure the message only once. There is no incentive to prevent others from replaying information

or from reusing stolen signatures. The described systems are not susceptible to such attacks on the information discussed in the references.

Finally, Applicants note that the limitations of a one-way hash function having... a system key as input, said system key not being shared with a remote electronic messaging system," has been completely ignored in the present Office action from the Examiner.

Accordingly, Applicants submit that Claims 1-22 are allowable over the references. First, many of the recited limitations are not present in either reference. Second, there is no motivation in the references to modify their teachings to obtain the missing limitations.
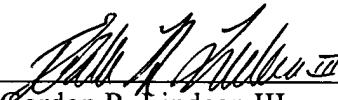
Conclusion

Applicants respectfully request the claims be allowed.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any

issue with allowance of the case.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: __1/27/4__

Gordon R. Lindeen III
Reg. No. 33,192

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1026
(303) 740-1980